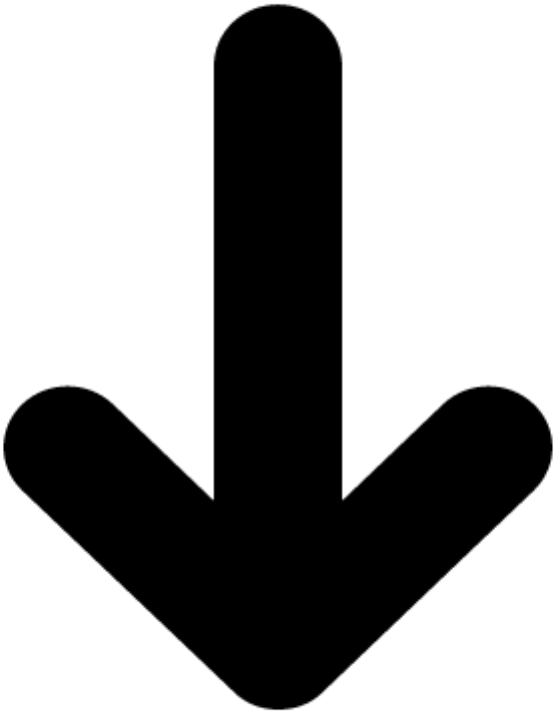
Proyek 6: Implementasi IDS (Intrusion Detection System) dengan Snort / Suricata

Nama Kelompok :

- 2201020098 Muhammad Rifqi
- 2201020123 Handicap
- 2201020139 Muhammad Iqbal Hordani
- 2201020101 Irsyad Widiansyah



Tahapan 3: Simulasi port scanning dengan nmap

- Port Scanning

Port scanning adalah teknik untuk memeriksa port-port yang terbuka pada suatu host atau server.
Tujuan scanning ini adalah untuk:

- mengidentifikasi layanan (service) yang berjalan,
- mengetahui port mana yang terbuka atau tertutup,
- memetakan potensi celah keamanan pada sistem.

Dalam konteks keamanan jaringan, port scan merupakan aktivitas yang sering dilakukan oleh penyerang (attacker) untuk mengumpulkan informasi sebelum melakukan serangan lebih lanjut. Oleh karena itu, Intrusion Detection System (IDS) seperti Suricata harus mampu mendeteksi pola scanning tersebut.

- Nmap

Nmap adalah singkatan dari **Network Mapper**, yaitu alat pemindai jaringan berbasis **opensource** yang digunakan untuk menemukan perangkat, port terbuka, dan layanan yang berjalan dalam suatu jaringan komputer. Nmap berfungsi untuk eksplorasi jaring an dan audit keamanan, serta membantu dalam mengidentifikasi potensi kerentanan d alam sistem jaringan. Alat ini sangat populer di kalangan profesional keamanan infor masi dan digunakan untuk berbagai tujuan, termasuk pemetaan jaringan dan pengujia n penetrasi.

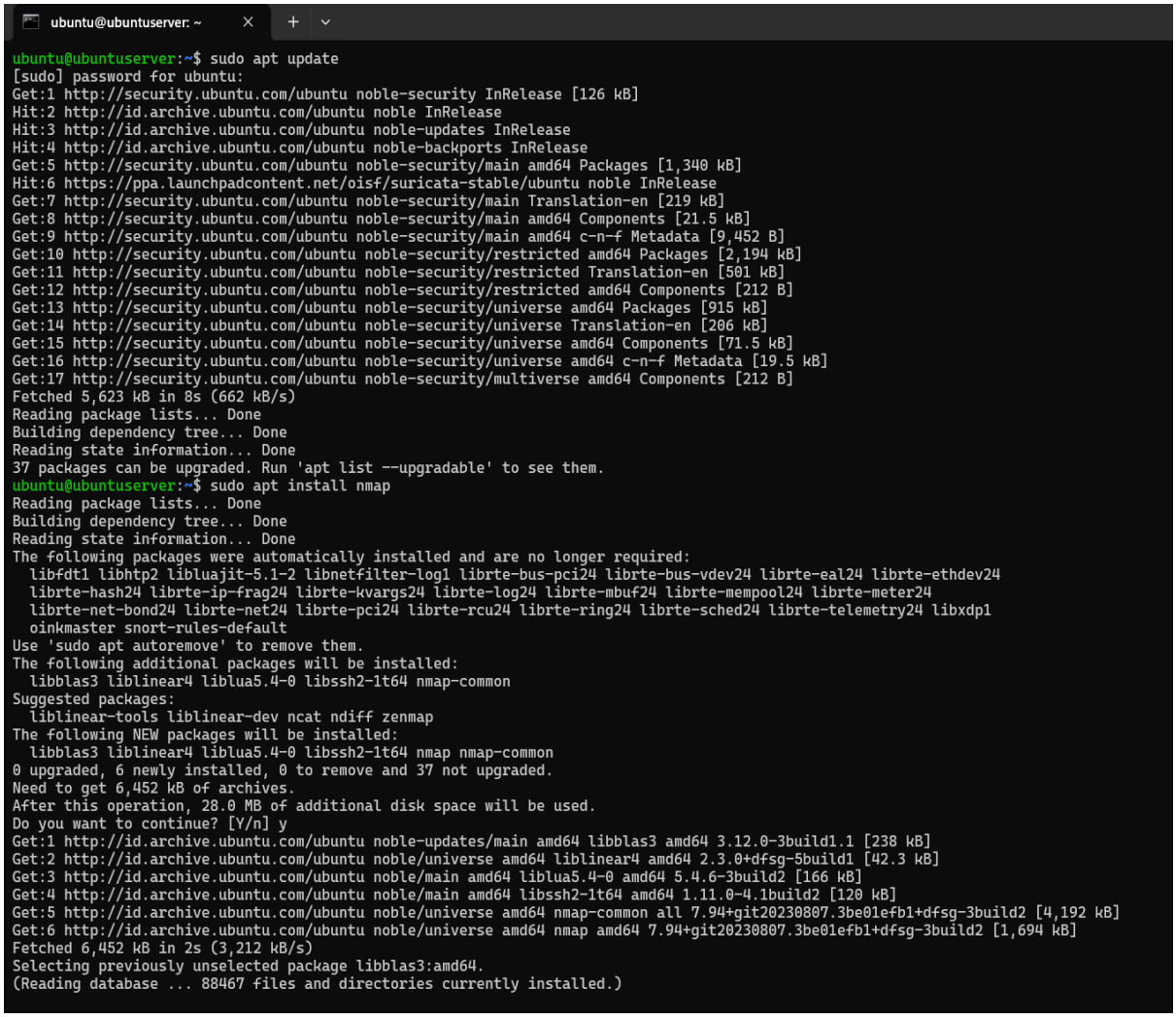
- Tujuan Simulasi

1. Menghasilkan aktivitas port scanning dari mesin attacker menggunakan Nmap
2. Memvalidasi apakah Suricata dapat mendeteksi pola scan tersebut
3. Menghasilkan log yang dapat dianalisis pada tahap selanjutnya

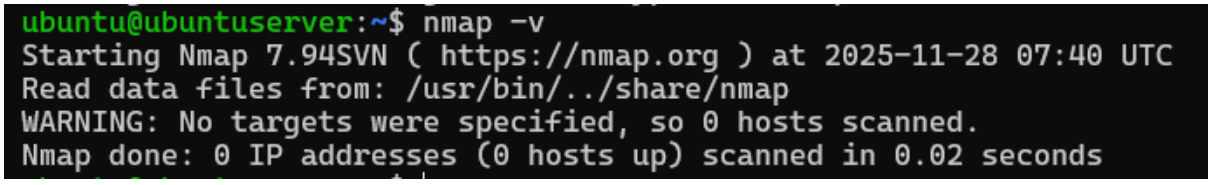
Dengan melakukan simulasi ini, mahasiswa dapat memahami bagaimana IDS mendeteksi pola scanning melalui rule bawaan Suricata.

Proggres

1. Install Nmap
    - sudo apt update
    - sudo apt install nmap



- cek instalasi Nmap : nmap -v



2. Simulasi Port Scanning dengan Nmap, Ip target = 192.168.56.102
   - Normal scan

     Normal scan adalah metode scanning standar Nmap yang digunakan untuk memeriksa port mana saja yang terbuka pada target. Scan ini mengirimkan paket TCP ke beberapa port umum dan menampilkan status port seperti **open**, **closed**, atau **filtered**.

     Perintah : nmap <IP_Target>

```
ubuntu@ubuntuserver:~$ nmap 192.168.56.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-11-28 07:52 UTC
Nmap scan report for 192.168.56.102 (192.168.56.102)
Host is up (0.000045s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 1 IP address (1 host up) scanned in 0.05 seconds
```

     Output :

     - **Host is up** → Artinya IP tersebut aktif dan bisa dijangkau.
     - **Not shown: 999 closed ports** → Ada 999 port yang tertutup.
     - **22/tcp open ssh** → Port **22 (SSH)** terbuka.

   - SYN scan (Stealth Scan)

     SYN scan adalah jenis scanning yang hanya mengirim paket **SYN** tanpa menyelesaikan proses handshake TCP.Teknik ini sering digunakan penyerang karena lebih cepat, lebih “diam-diam”, dan sering tidak tercatat oleh service target.IDS seperti Suricata biasanya mendeteksi scan ini sebagai aktivitas mencurigakan.

     Perintah : sudo nmap -sS <IP_Target>

```
ubuntu@ubuntuserver:~$ sudo nmap -sS 192.168.56.102
[sudo] password for ubuntu:
Sorry, try again.
[sudo] password for ubuntu:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-11-28 07:56 UTC
Nmap scan report for 192.168.56.102 (192.168.56.102)
Host is up (0.0000060s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 1 IP address (1 host up) scanned in 0.12 seconds
```

     Output :

     - **Host is up** → Target aktif.
     - **Not shown: 999 closed tcp ports (reset)** → Artinya 999 port mengirimkan respon **RST**, menunjukkan port tertutup.
     - **22/tcp open ssh** → Port 22 terdeteksi **open**.

- Aggressive scan (-A Scan)

  Aggressive scan melakukan scanning yang lebih lengkap:

  - mendeteksi versi service
  - identifikasi sistem operasi (OS detection)
  - melakukan traceroute
  - scanning port secara menyeluruh

  Metode ini menghasilkan traffic lebih banyak dan mudah terdeteksi oleh IDS.

  Perintah : sudo nmap -A <IP_Target>

```
ubuntu@ubuntuserver:~$ sudo nmap -A 192.168.56.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-11-28 07:59 UTC
Nmap scan report for 192.168.56.102 (192.168.56.102)
Host is up (0.000038s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 9.6p1 Ubuntu 3ubuntu13.14 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 c4:4c:c7:1d:ba:9c:c7:fb:d6:a4:2f:0e:85:08:06:9c (ECDSA)
|_  256 f3:b9:a4:4c:bb:af:9d:97:0f:03:ae:21:69:e9:43:6f (ED25519)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6.32
OS details: Linux 2.6.32
Network Distance: 0 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.93 seconds
ubuntu@ubuntuserver:~$
```

Output :

- **Target IP:** 192.168.56.102
- **Host Status:** Up
- **Port Terbuka:**
  - **22/tcp – OpenSSH 9.6p1 (Ubuntu)**
- **SSH Host Key:**
  - Terdeteksi fingerprint ECDSA & ED25519
- **OS Detection:**
  - Sistem operasi teridentifikasi sebagai **Linux kernel 2.6.x**
- **Device Type:**
  - General purpose (mesin komputer umum)
- **Network Distance:** 0 hops (satu jaringan / langsung)
- **Waktu Scan:** ~1.93 detik